Forcing on three sort bounded arithmetic and related theories (Proof theory and related topics)

AUTHOR(S):

Kuroda, Satoru

CITATION:

Kuroda, Satoru. Forcing on three sort bounded arithmetic and related theories (Proof theory and related topics). 数理解析研究所講究録 2020, 2150: 41-55

ISSUE DATE:

2020-04

URL:

http://hdl.handle.net/2433/255055

Forcing on three sort bounded arithmetic and related theories

Satoru Kuroda*
Department of Liberal Arts,
Gunma Prefectural Women's University

Abstract

In this paper, we apply forcing method for Bounded Arithmetic which was developed by G. Takeuti and M. Yasumoto to three sort theories. As a result, we obtain generic extensions which are models of a minimal theory for PSPACE. Proofs are sketchy and full length proofs will be given in the paper which is in preparation. We also present some problems and ideas for the future research.

1 A brief (not exhaustive) history of Bounded Arithmetic

Since the seminal papers by Cook [6] and Buss [3], bounded arithmetic have been considered in the context of computational complexity as well as proof complexity.

In 1975, Cook gave a weak system of arithmetic PV which have all polynomial time functions and showed that it is related to extended Frege proofs. Then Buss defined a hierarchy S^i_2 and T^i_2 which corresponds to the polynomial time hierarchy in the sense that

Theorem 1 (Buss [3]) *A function is Σ^b_i definable in S^i_2 or T^{i+1}_2 if and only if it is computable in polynomial time with oracles from Σ^p_i.*

This result suggests that separation problems of theories of bounded arithmetic are closely connected to separation problems of complexity classes. This connection was soon given in more formal manner as a consequence of the KPT witnessing theorem [8] as follows:

Theorem 2 (Buss [4], Zambella [20]) *Let $i \geq 1$, if $T^i_2 = S^{i+1}_2$ the T^i_2 proves that the polynomial hierarchy collapses. For $i = 0$ the same holds for PV instead of T^0_2.*

After Buss' thesis, a number of theories are proposed for other complexity classes. In particular several weak fragments of Buss' theories are defined for subclasses of PTIME [5]. However, compared to Buss' systems which are axomatized by weak forms of induction, these theories have rather unintuitive axioms which are hard to investigate.

*This work was supported by JSPS KAKENHI Grant Number 18K03400.

This inefficiency was overcome by Cook and Nugyen [7] who established the theory of two-sort bounded arithmetic and proposed various theories for subP classes. In two-sort bounded arithmetic, there are two sorts of objects, namely natural numbers and binary strings. Binary strings are used to code computations of Turing machines, Boolean circuits and so on and numbers are mainly used to denote the length of inputs and calculate resources required for the computation.

The base theory is $\mathbf{V}^0$ which corresponds to the class AC^0 and for many subP complexity classes $\mathcal{C}$, corresponding theory $V\mathcal{C}$ is obtained by adding to $\mathbf{V}^0$ a single axiom which represents a complete problem for the class.

Turning to stronger complexity classes, Buss' thesis already defined second order theories which corresponds to PSPACE and EXPTIME hierarchy. For the class PSPACE, it is possible to construct corresponding theories in two-sort language [12]. Another interesting formulation is proposed by Skelley [16] who established a three-sort language and defined a theory W_1^1 whose provably total functions are exactly those computable in PSPACE.

Skelley added third sort of objects, namely superstrings (sets of strings) in order to code computations of PSPACE machines. In theories in three sort language, there is no way to compute the length a given superstring, yet elements can be recognized as far as they are in polynomial range.

As a result, this formulation enables to construct theories with objects with exponential size while prohibiting the totality of the exponentiation.

2 A brief history of forcing in bounded arithmetic

The application of forcing methods in bounded arithmetic was initiated by Paris and Wilkie [14]. For a L-theory T and a new relation symbol R, $T(R)$ denotes the $L(R)$-theory whose axioms are those for T relativized by the language $L(R)$. Then Paris and Wilkie showed that

Theorem 3 (Paris and Wilkie [14]) *The theory $IE_1(R)$ cannot prove that R is a bijection from $n+1$ to n.*

In their proof, the bijection $R : n+1 \to n$ is constructed using a similar manner as in the cardinal collapsing in set theoretic forcing.

After that, Ajtai [1] made a great leap forward. Specifically, he showed that

Theorem 4 (Ajtai [1]) *The theory $I\Delta_0(R)$ cannot prove that R is a bijection from $n+1$ to n.*

Although the construction of the bijection is similar to the result by Paris and Wilkie, the proof of Ajtai's result requires a complicated argument of probabilistic combinatorics.

After Ajtai's result, Riis [15] gave similar forcing construction for Buss' theories which is recently extended by Atserias and Müller [2] and Müller [13].

Another type of forcing construction in bounded arithmetic was given by Krajíček. His line of research is to obtain nonstandard models of weak theories which settle separation problems such as $P \neq NP$ or problems in proof complexity. Specifically, he used forcing methods to obtain the following results:

Theorem 5 (Krajíček [10]) *Let $M \models PV$ and suppose that $M \models NP \not\subseteq P/poly$. Then there exists a Π_1^B elementary extension $M' \models PV + NP \not\subseteq co\text{-}NP/poly$.*

Theorem 6 (Krajíček [9]) *Let $M \models \mathbf{V}^1$ and suppose that a there exists a propositional formula $\tau \in M$ which does not have a EF proof in M. Then there exists an extension $M' \models \mathbf{V}^1$ in which $\neg\tau$ is satisfiable.*

The third wave of forcing in bounded arithmetic was presented by Takeuti and Yasumoto [18], [19]. They gave a forcing construction from a Boolean algebra which consists of Boolean circuits in the ground model. Then they showed that the generic extension so constructed relates to the separation problem of complexity classes.

In the rest of the paper we construct generic extensions of three-sort structures. Specifically, we will construct a generic extension from a given countable nonstandard model of W_1^1 using a similar argument as in Takeuti and Yasumoto.

3 Preliminaries

In this section we briefly review three-sort bounded arithmetic in [16] and define a new minimal theory for PSPACE.

We deal with theories and structures in three sort language $\mathcal{L}_A^3$. The language $\mathcal{L}_A^3$ comprises three sort of variables

- number variables :$x, y, z, \ldots$
- string variables :$X, Y, Z, \ldots$
- superstring variables :$\mathcal{X}, \mathcal{Y}, \mathcal{Z}, \ldots$

and the following function symbols and predicate symbols:

$$Z() = 0, s(x) = x + 1, x + y, x \cdot y, |X|, x \in_2 Y, X \in_3 \mathcal{Y}.$$

$\Sigma_0^{\mathcal{B}}$ is the set of $\mathcal{L}_A^3$ formulas in which all quantifiers are either bounded number quantifiers or bounded string quantifiers. $\Sigma_1^{\mathcal{B}}$ is the set of $\mathcal{L}_A^3$ formulas which are logically equivalent to formulas of the form

$$\exists \mathcal{Y}\, \varphi(\bar{x}, \bar{X}, \bar{\mathcal{X}}, \mathcal{Y})$$

where $\varphi(\bar{x}, \bar{X}, \bar{\mathcal{X}}, \mathcal{Y}) \in \Sigma_0^{\mathcal{B}}$. $\forall^2\Sigma_1^{\mathcal{B}}$ is the set of formulas of the form

$$\forall Y_1 < t_1 \cdots Y_k < t_k\, \varphi(\bar{x}, \bar{X}, \bar{Y}, \bar{\mathcal{X}})$$

where $\varphi(\bar{x}, \bar{X}, \bar{Y}, \bar{\mathcal{X}}) \in \Sigma_1^{\mathcal{B}}$.

We define theories for three sort as follows.

Definition 1 *W_1^0 is the $\mathcal{L}_A^3$-theory whose axioms are:*

- *the finite set of axioms $BASIC_3$ which define symbols in $\mathcal{L}_A^3$.*
- *$\Sigma_0^{\mathcal{B}}$-2COMP*
$$\exists Y \, \forall x < a \, (Y(x) \leftrightarrow \varphi(x))$$
where $\varphi(x) \in \Sigma_0^{\mathcal{B}}$ does not contain Y.
- *$\Sigma_0^{\mathcal{B}}$-3COMP*
$$\exists \mathcal{Y} \, \forall X < a \, (\mathcal{Y}(X) \leftrightarrow \varphi(X))$$
where $\varphi(X) \in \Sigma_0^{\mathcal{B}}$ does not contain $\mathcal{Y}$.

W_1^1 is the theory W_1^0 extended by $\forall^2\Sigma_1^{\mathcal{B}}$-3COMP.

Theorem 7 (Skelley [16]) *A function is $\Sigma_1^{\mathcal{B}}$ definable in W_1^1 if and only if it is in $FPSPACE^+$.*

We define another theory which is obtained by extending W_1^0 by a single axiom which represents a PSPACE complete problem.

QBF games is the game played by two players on a quantified Boolean formulas. Let

$$\exists x_1 \forall y_1 \cdots \exists x_l \forall y_l \phi(x_1, \ldots, x_l, y_1, \ldots, y_l)$$

be a quantified Boolean formula. Players 1 and 2 in turn chooses assignments for x_i and y_i for $1 \leq i \leq l$. Player 1 wins if the assignments satisfy ϕ and Player 2 wins otherwise.

It is well-known that computing winning strategies for QBF games is PSPACE complete. We can formalize strategies by superstirngs. define

$$Assign1(l, X, Y, \mathcal{T}) \leftrightarrow |X| = |Y| = l \wedge \forall z < l \, (X(z) \leftrightarrow \mathcal{T}(Y \restriction_z)$$

and

$$Assign2(l, X, Y, \mathcal{F}) \leftrightarrow |X| = |Y| = l \wedge \forall z < l \, (Y(z) \leftrightarrow \mathcal{F}(X \restriction_z)$$

Then define

$$True(l, \eta) \Leftrightarrow \exists \mathcal{T} \, \forall X, Y < l \, (Assign1(l, X, Y, \mathcal{T}) \rightarrow \langle X, Y \rangle \models \eta)$$

and

$$False(l, \eta) \Leftrightarrow \exists \mathcal{F} \, \forall X, Y < l \, (Assign2(l, X, Y, \mathcal{F}) \rightarrow \langle X, Y \rangle \not\models \eta).$$

Finally define

$$Ax\text{-}QBF \equiv \forall l \, \forall \eta \, (True(l, \eta) \vee False(l, \eta)).$$

and

$$\mathbf{QBFV} = W_1^0 + Ax\text{-}QBF.$$

By a standard witnessing argument, we have

Theorem 8 *A function is $\Sigma_1^{\mathcal{B}}$-definable in* **QBFV** *if and only if it is in FPSPACE.*

Corollary 1 *W_1^1 is a $\forall\Sigma_1^{\mathcal{B}}$ extension of* **QBFV**.

4 Three-sort Generic extensions

Throughout the paper, we assume that $\mathfrak{M} = \langle M_0, M, \mathcal{M}\rangle$ is a countable and nonstandard $\mathcal{L}_A^3$-structure.

Let $BP \subseteq M$ be the set of Boolean programs in $\mathfrak{M}$. Formally, BP consists of sequences of the form $\langle C_0, \ldots, C_l\rangle$ such that each C_i is a formula with connectives from

$$\wedge, \vee, \neg, f_0, \ldots, f_{i-1}.$$

where the arity of f_i is equal to the number of propositional variables in C_i.

Let $n \in M_0 \setminus \omega$ and $\bar{p} = p_0, \ldots, p_{n-1}$ be a list of propositional variables in $\mathfrak{M}$ and define

$$BP(\bar{p}) = \{\langle C_0, \ldots, C_l\rangle \in BP : \text{propositional variables of } C_l \text{ are among } \bar{p}\}.$$

It is readily seen that there exists a $\Sigma_0^{\mathcal{B}}$ formula

$$BooleP(X, \bar{p}) \Leftrightarrow X \in BP(\bar{p}).$$

Note that we can naturally introduce Boolean operations in $\mathbb{B}_{BP}$. So we regard $\mathbb{B}_{BP}$ as a Boolean algebra.

We define a $\Delta_1^{\mathcal{B}}$ formula

$$\alpha \models_{BP} X \Leftrightarrow (\alpha \in 2^n \wedge X \in BP(\bar{p}) \wedge X \text{ evaluates to true on } \alpha).$$

For $X, Y \in BP(\bar{p})$ define

$$X \leq_{BP} Y \Leftrightarrow \forall A \in 2^n \, (A \models_{BP} X \to A \models_{BP} Y)$$

and

$$X =_{BP} Y \Leftrightarrow X \leq_{BP} Y \wedge Y \leq_{BP} X.$$

Finally define

$$\mathbb{B}_{BP} = BP(\bar{p})/ =_{BP}.$$

We can alternatively define another partial order on $BP(\bar{p})$ based on propositional provability. Let BPLK be the proof system LK operated on Boolean programs (cf. [16]) and define

$$X \leq_{BPLK} Y \Leftrightarrow \mathfrak{M} \models \exists P \, (P \text{ is a BPLK-proof of } Y \text{ from } X).$$

In the following argument, we assume that $\mathbb{B} = \mathbb{B}_{BP}$ unless otherwise stated.

A set $\mathbb{I} \subseteq \mathbb{B}$ is an ideal if $0 \in \mathbb{I}$, $1 \notin \mathbb{I}$, closed under $\vee$ and downward closed with respect to $\leq_{BP}$.

An ideal $\mathbb{I} \subseteq \mathbb{B}$ is M_0-complete if for any $X \in M$ with $X : k \to \mathbb{B}$,

$$X_i \in \mathbb{I} \text{ for some } i < k \Rightarrow \bigvee_{i<k} C_i \in \mathbb{I}.$$

A set $\mathbb{G} \subseteq \mathbb{B}$ is a filter if $0 \notin \mathbb{G}$, $1 \in \mathbb{G}$, closed under $\wedge$ and upward closed with respect to $\leq_{BP}$.

A filter $\mathbb{G} \subseteq \mathbb{B}$ is maximal if exactly one of $X \in \mathbb{G}$ or $\neg X \in \mathbb{G}$ is true for any $X \in \mathbb{B} \setminus \mathbb{I}$.

A set $\mathbb{D} \subseteq \mathbb{B}$ is dense over an M_0-complete ideal $\mathbb{I}$ if for any $X \in \mathbb{B} \setminus \mathbb{I}$ there exists $Y \in \mathbb{D} \setminus \mathbb{I}$ such that $Y \leq X$.

A maximal filter is a TY-generic over an M_0-complete ideal $\mathbb{I}$ if it intersects with any dense set over $\mathbb{I}$.

The following can be proved by a similar argument as in set theory.

Proposition 1 *Let $\mathbb{I} \subseteq \mathbb{B}$ be an M_0-complete ideal. For any $X \in \mathbb{B} \setminus \mathbb{I}$ there exists a TY-generic $\mathbb{G}$ over $\mathbb{I}$ such that $X \in \mathbb{G}$.*

As in set theory, we define names for the string part and the superstring part. Specifically, define

$$M^{\mathbb{B}} = \{X \in M : X : a \to \mathbb{B} \text{ for some } a \in M_0\}$$

and

$$\mathcal{M}^{\mathbb{B}} = \{\mathcal{X} \in \mathcal{M} : X : M^{\mathbb{B}} \to \mathbb{B}\}.$$

For $\mathcal{X} \in \mathcal{M}^{\mathbb{B}}$, we denote its domain by $dom(\mathcal{X})$.

Now we can define the genric extension. Let $\mathbb{G} \subseteq \mathbb{B}$ be a TY-generic. For $X \in M^{\mathbb{B}}$ with $X : a \to \mathbb{B}$, we define

$$X_{\mathbb{G}} = \{i < a : X(i) \in \mathbb{G}\}.$$

For $\mathcal{X} \in \mathcal{M}^{\mathbb{B}}$, we define

$$\mathcal{X}_{\mathbb{G}} = \{X_{\mathbb{G}} : \mathcal{X}(X) \in \mathbb{G}\}.$$

Define

$$M_{\mathbb{G}} = \{X_{\mathbb{G}} : X \in M^{\mathbb{B}}\}, \qquad \mathcal{M}_{\mathbb{G}} = \{\mathcal{X}_{\mathbb{G}} : \mathcal{X} \in \mathcal{M}^{\mathbb{B}}\}.$$

Finally, define

$$\mathfrak{M}[\mathbb{G}] = (M_0, M_{\mathbb{G}}, \mathcal{M}_{\mathbb{G}}).$$

It turns out that the forcing theorem holds for $\Sigma_0^{\mathcal{B}}$ formulas. For the proof, we need to define Boolean values.

Definition 2 *For $\varphi(\bar{x}, \bar{X}, \bar{\mathcal{X}}) \in \Sigma_0^{\mathcal{B}}$, $\bar{a} \in M_0$, $\bar{A} \in M^{\mathbb{B}}$ and $\bar{\mathcal{A}} \in \mathcal{M}^{\mathbb{B}}$ we define the Boolean program $[\![\varphi(\bar{x}, \bar{X}, \bar{\mathcal{X}})]\!] \in \mathbb{B}$ inductively as follows:*

- *if s and t be a term with parameters from $\mathfrak{M}$ then*

$$[\![s = t]\!] = \begin{cases} 1, & \text{if } \mathfrak{M} \models s = t, \\ 0, & \text{otherwise.} \end{cases}$$

- *If $b \in M_0$ and $A : a \to \mathbb{B}$ then*

$$[\![b \in A]\!] = \begin{cases} A(b), & \text{if } b < a, \\ 0, & \text{otherwise.} \end{cases}$$

- *If $B \in M_0$ and $\mathcal{A} \in \mathcal{M}^{\mathbb{B}}$ then*

$$[\![B \in \mathcal{A}]\!] = \begin{cases} \mathcal{A}(B), & \text{if } B \in dom(\mathcal{A}), \\ 0, & \text{otherwise.} \end{cases}$$

- $[\![\varphi \wedge \psi]\!] = [\![\varphi]\!] \wedge [\![\psi]\!]$, $[\![\varphi \vee \psi]\!] = [\![\varphi]\!] \vee [\![\psi]\!]$ *and* $[\![\neg\varphi]\!] = \neg[\![\varphi]\!]$.
- *If t is a term then*

$$[\![\exists x < t\varphi(x)]\!] = \bigvee_{x<t} [\![\varphi(x)]\!], \quad [\![\forall x < t\varphi(x)]\!] = \bigwedge_{x<t} [\![\varphi(x)]\!].$$

- $[\![\exists X \leq t\ \varphi(X)]\!]$ *consists of the following formulas:*

$$\begin{array}{l} \phi_{l,0}(q_0, \ldots, q_l) = [\![\varphi(\langle q_0, \ldots, q_l\rangle)]\!], \\ \phi_{l,i}(q_i, \ldots, q_l) = \phi_{l,i-1}(0, q_i, \ldots, q_l) \vee \phi_{l,i-1}(1, q_i, \ldots, q_l), \\ \phi = \bigvee_{l \leq t} \phi_{l,l+1}. \end{array}$$

- $[\![\forall X \leq t\ \varphi(X)]\!]$ *consists of the following formulas:*

$$\begin{array}{l} \phi_{l,0}(q_0, \ldots, q_l) = [\![\varphi(\langle q_0, \ldots, q_l\rangle)]\!], \\ \phi_{l,i}(q_i, \ldots, q_l) = \phi_{l,i-1}(0, q_i, \ldots, q_l) \wedge \phi_{l,i-1}(1, q_i, \ldots, q_l), \\ \phi = \bigwedge_{l \leq t} \phi_{l,l+1}. \end{array}$$

It is easy to see that the Boolean translation $[\![\cdot]\!]$ satisfies the following basic properties:

Lemma 1 *The translation $[\![\cdot]\!]$ satisfies the DeMorgan law. That is for any $\varphi(X) \in \Sigma_0^{\mathcal{B}}$ and a term t,*

$$[\![\forall X \leq t\ \varphi(X)]\!] =_{BP} [\![\neg\exists X \leq t\ \neg\varphi(X)]\!] \text{ and}$$
$$[\![\exists X \leq t\ \varphi(X)]\!] =_{BP} [\![\neg\forall X \leq t\ \neg\varphi(X)]\!].$$

Lemma 2 *For any $\varphi(X) \in \Sigma_0^{\mathcal{B}}$ with parameters, a term t and $A \in 2^n$, $A \models_{BP} [\![\exists X \leq t\varphi(X)]\!]$ if and only if there exists $B \in 2^t$ such that $\langle A, B\rangle \models_{BP} [\![\varphi(X)]\!]$ where X is interpreted by B. Similarly $A \models_{BP} [\![\forall X \leq t\varphi(X)]\!]$ if and only if for any $B \in 2^t$, $\langle A, B\rangle \models_{BP} [\![\varphi(X)]\!]$.*

Theorem 9 (Forcing Theorem) *Let* $\varphi(\bar{x}, \bar{X}, \bar{\mathcal{X}}) \in \Sigma_0^{\mathcal{B}}$, $\bar{a} \in M_0$, $\bar{A} \in M^{\mathbb{B}}$ *and* $\bar{\mathcal{A}} \in \mathcal{M}^{\mathbb{B}}$ *and* $\mathbb{G} \subseteq \mathbb{B}$ *be a TY-generic. Then*

$$\mathfrak{M}[\mathbb{G}] \models \varphi(\bar{a}, \overline{A_{\mathbb{G}}}, \overline{\mathcal{A}_{\mathbb{G}}}) \Leftrightarrow [\![\varphi(\bar{a}, \bar{A}, \bar{\mathcal{A}})]\!] \in \mathbb{G}.$$

Before proving Forcing Theorem, we prove a technical lemma:

Lemma 3 W_1^1 *proves that there exists a PSPACE function* $F(x, \phi)$ *such that for any Boolean program* $\phi(\bar{x}, \bar{z})$,

$$\exists Z < t \, \langle X, Z\rangle \models_{BP} \phi(\bar{x}, \bar{z}) \leftrightarrow \langle X, F(X, \phi)\rangle \models_{BP} \phi(\bar{x}, \bar{z}).$$

(Proof). We can construct F using binary search provably in W_1^1. □

(Proof Sketch of Theorem 9).

We prove the theorem by induction on φ. It suffices to prove the following cases since other cases are identical to the proof in [18].

Let $B \in M^{\mathbb{B}}$, $\mathcal{A} \in \mathcal{M}^{\mathbb{B}}$ and $B \in dom(\mathcal{A})$. Then

$$\mathfrak{M}[\mathbb{G}] \models B_{\mathbb{G}} \in \mathcal{A}_{\mathbb{G}} \quad \Leftrightarrow \quad B_{\mathbb{G}} \in \{A_{\mathbb{G}} : \mathcal{A}(A) \in \mathbb{G}\} \Leftrightarrow \mathcal{A}(B) \in \mathbb{G}.$$

Suppose that the claim holds for $\psi(\bar{a}, \bar{X}, Z, \bar{\mathcal{X}}) \in \Sigma_0^{\mathcal{B}}$ and let t be a term with parameters from $\bar{x}, \bar{X}$. By the inductive hypothesis, we have

$$\mathfrak{M}[\mathbb{G}] \models \exists Z \ \leq t \, \psi(\bar{a}, \bar{X_{\mathbb{G}}}, Z, \bar{\mathcal{X}_{\mathbb{G}}})$$

if and only if there exists $Z : t \to \mathbb{B}$ such that $[\![\psi(\bar{a}, \bar{X}, Z, \bar{\mathcal{X}})]\!] \in \mathbb{G}$. So it suffices to show that this condition holds if and only if

$$[\![\exists Z \leq t \, \psi(\bar{a}, \bar{X}, Z, \bar{\mathcal{X}})]\!] \in \mathbb{G}.$$

The only-if part is implied by the fact that for any $Z : t \to \mathbb{B}$,

$$[\![\psi(\bar{a}, \bar{X}, Z, \bar{\mathcal{X}})]\!] \leq_{BP} [\![\exists Z \leq t \, \psi(\bar{a}, \bar{X}, Z, \bar{\mathcal{X}})]\!]$$

which is a consequence of Lemma 2.

For if part we remark that

Lemma 4 *Let* $\psi(\bar{a}, \bar{X}, Z, \bar{\mathcal{X}}) \in \Sigma_0^{\mathcal{B}}$ *and* t *be a term with parameters from* $\bar{x}, \bar{X}$. W_1^1 *proves that there exists a family* $\bar{C_n}$ *of Boolean programs such that*

$$\begin{aligned}\forall n \, \forall A \in 2^n \, (A \models_{BP} [\![\exists Z \leq t \, \psi(\bar{a}, \bar{X}, Z, \bar{\mathcal{X}})]\!] \\ \leftrightarrow \langle A, \bar{C_n}(\bar{x}, \bar{X}, \bar{\mathcal{X}})\rangle \models_{BP} [\![\psi(\bar{a}, \bar{X}, Z, \bar{\mathcal{X}})]\!]),\end{aligned}$$

where in the LHS of the equivalence, Z *is interpreted by* $\bar{C_n}(\bar{x}, \bar{X}, \bar{\mathcal{X}})$.

(Proof Sketch of Lemma 4).

We can use binary search to find a witness B such that

$$|B| \leq t \wedge \langle A, B\rangle \models_{BP} [\![\psi(\bar{a}, \bar{X}, Z, \bar{\mathcal{X}})]\!]$$

using the BP to check $[\![\psi(\bar{a}, \bar{X}, Z, \bar{\mathcal{X}})]\!]$. Moreover, such an algorithm is easily transformed into BPs. □

Now we can finish the proof of forcing theorem. Let $\bar{C_n} = \langle C_{n,0}, \ldots, C_{n,t}\rangle$ be the list of BPs given in Lemma 4 and define

$$C : t \to \mathbb{B}, \quad C(i) = C_{n,i}(\bar{x}, \bar{X}, \bar{\mathcal{X}}).$$

Then Lemma 4 shows that

$$[\![\exists Z \leq\ t\psi(\bar{a}, \bar{X}, Z, \bar{\mathcal{X}})]\!] \leq_{BP} [\![\psi(\bar{a}, \bar{X}, C, \bar{\mathcal{X}})]\!]$$

which completes the proof. □(Theorem 9)

Theorem 10 *If* $\mathfrak{M} \models W_1^1$ *and* $\mathbb{G} \in \mathbb{B}$ *is a TY-generic then* $\mathfrak{M}[\mathbb{G}] \models W_1^0$.

(Proof). It suffices to show that $\mathfrak{M}[\mathbb{G}]$ satisfies $\Sigma_0^{\mathcal{B}}$-3COMP. Let $\varphi(\bar{x}, X, \bar{Y}, \bar{\mathcal{X}}) \in \Sigma_0^{\mathcal{B}}$, $a, \bar{b} \in M_0$, $\bar{A} \in M^{\mathbb{B}}$ and $\bar{\mathcal{A}} \in \mathcal{M}^{\mathbb{B}}$. Define

$$\mathcal{Z} = \{\langle X, [\![\varphi(\bar{b}, X, \bar{A}, \bar{\mathcal{A}})]\!]\rangle : X \in M^{\mathbb{B}},\ X : x \to \mathbb{B} \text{ for some } x < a\}.$$

By Theorem 9, it is readily shown that

$$\mathfrak{M}[\mathbb{G}] \models \forall X < a\ (X \in \mathcal{Z}_{\mathbb{G}} \leftrightarrow \varphi(\bar{b}, X, \bar{Y_{\mathbb{G}}}, \bar{\mathcal{X}_{\mathbb{G}}})).$$

Since the Boolean algebra $\mathbb{B}_{BP}$ is based on the computation model for PSPACE, we expect that the generic extension is at least closed under PSPACE functions. Next, we will show that this is in fact the case.

Theorem 11 *If* $\mathfrak{M} \models W_1^1$ *and* $\mathbb{G} \subseteq \mathbb{B}$ *is a TY-generic then* $\mathfrak{M}[\mathbb{G}] \models \mathbf{QBFV}$.

(Proof Sketch). First we remark that computing stategies for QBF games is in PSPACE provably in W_1^1. Let $\eta \in M$ be a QBF with $2l$ variables. Then there exists Boolean programs $C_a, D_a \in M$ for $a < l$ such that

$$\forall X, Y\ (|X| = |Y| = l \wedge \forall z < l\ (X(z) \leftrightarrow C_z(Y\restriction_z) = 1 \to \langle X, Y\rangle \models \eta))$$

or

$$\forall X, Y\ (|X| = |Y| = l \wedge \forall z < l\ (Y(z) \leftrightarrow D_z(X\restriction_z) = 1 \to \langle X, Y\rangle \not\models \eta))$$

hold in $\mathfrak{M}$.

For $X, Y : a \to \mathbb{B}$, set

$$C_Y = C_a(Y), \quad D_X = D_a(X)$$

and define $\mathcal{T}, \mathcal{F} \in \mathcal{M}^{\mathbb{B}}$ as

$$\mathcal{T} = \{\langle Y, C_Y\rangle : Y \in M^{\mathbb{B}}, Y : a \to \mathbb{B} \text{ for some } a < l\},$$
$$\mathcal{F} = \{\langle X, D_X\rangle : X \in M^{\mathbb{B}}, X : a \to \mathbb{B} \text{ for some } a < l\}.$$

Claim. Either one of the followings holds in $\mathfrak{M}$:

1. for any $X, Y : l \to \mathbb{B}$,

$$\left(\bigwedge_{z<l} (X(z) \leftrightarrow \mathcal{T}(Y\restriction_z)) \to [\![\langle X, Y\rangle \models \eta]\!]\right) =_{BP} 1.$$

2. for any $X, Y : l \to \mathbb{B}$,

$$\left(\bigwedge_{z<l} (Y(z) \leftrightarrow \mathcal{F}(X\restriction_z)) \to [\![\langle X, Y\rangle \not\models \eta]\!]\right) =_{BP} 1.$$

This claim is implied from the fact that in $\mathfrak{M}$, Ax-QBF is true and is witnessed by C_a and D_a.

Now from 1 of Claim, we obtain that for $X, Y : l \to \mathbb{B}$,

$$\bigwedge_{z<l} (X(z) \leftrightarrow \mathcal{T}(Y\restriction_z)) \in \mathbb{G} \Rightarrow [\![\langle X, Y\rangle \models \eta]\!] \in \mathbb{G}$$

which implies that

$$\mathfrak{M}[\mathbb{G}] \models \forall X, Y\ (Assign1(X, Y, \mathcal{T}_{\mathbb{G}}) \to \langle X, Y\rangle \models \eta_{\mathbb{G}}).$$

Similarly, from 2 of Claim, we obtain that for an $X, Y : l \to \mathbb{B}$,

$$\bigwedge_{z<l} (Y(z) \leftrightarrow \mathcal{F}(X\restriction_z)) \in \mathbb{G} \Rightarrow [\![\langle X, Y\rangle \not\models \eta]\!] \in \mathbb{G}$$

which implies that

$$\mathfrak{M}[\mathbb{G}] \models \forall X, Y\ (Assign2(X, Y, \mathcal{T}_{\mathbb{G}}) \to \langle X, Y\rangle \not\models \eta_{\mathbb{G}}).$$

Thus we have proved the claim of the theorem. □

Corollary 2 *If $\mathfrak{M} \models W_1^1$ and $\mathbb{G} \subseteq \mathbb{B}$ is a TY-generic then $\mathfrak{M}[\mathbb{G}] \models \forall \Sigma_1^{\mathcal{B}}(W_1^1)$.*

5 Some remarks

We finish the paper by giving some miscellaneous results on three sort forcing together with ideas for future works.

5.1 When generic is an element of generic extension

Under some assumption, we can regard generic $\mathbb{G} \subseteq \mathbb{B}$ as a superstring of the generic extension $\mathfrak{M}[\mathbb{G}]$. This is unlike the case for two-sort generic extensions.

Definition 3 *The Boolean algebra $\mathbb{B}$ based on the set $BP(\bar{p}) \subseteq M$ is bounded in $\mathfrak{M}$ if there exists a term $t(n)$ such that*

$$\mathfrak{M} \models \forall X \in BP(\bar{p})\ \exists Y \in BP(\bar{p})\ (|Y| < t(n) \wedge X =_{BP} Y).$$

Theorem 12 *Let $\mathfrak{M} \models W_1^1$. If $\mathbb{B}$ is bounded then for any TY-generic $\mathbb{G} \subseteq \mathbb{B}$, $\mathbb{G} \in \mathcal{M}_{\mathbb{G}}$.*

(Proof). Suppose that $\mathbb{B}$ is bounded by the term $t(n)$. Then by $\Sigma_0^{\mathcal{B}}$-3COMP in $\mathfrak{M}$, we have

$$\mathcal{B} = \{X \in M : X \in BP(\bar{p}) \wedge |X| \leq t(n)\} \in \mathcal{M}.$$

Define

$$\mathcal{G} = \{\langle \check{X}, X\rangle : X \in \mathcal{B}\} \in \mathcal{M}^{\mathbb{B}}.$$

Then it is easy to see that $\mathcal{G}_{\mathbb{G}} = \mathbb{G}$. □

Corollary 3 *For $k \in \omega$, let BP_k be the class of languages which are decidable by Boolean programs wich size bounded by $O(n^k)$. If*

$$\mathfrak{M} \models W_1^1 + PSPACE \subseteq BP(k)$$

then $\mathbb{G} \in \mathfrak{M}[\mathbb{G}]$ whenever $\mathbb{G} \subseteq \mathbb{B}$ is a TY-generic.

The idea behind Corollary 3 comes from the result of Santhanam and Williams which states that

Theorem 13 (Santhanam and Williams [17]) *For any $k \in \omega$, $P \not\subseteq Size(n^k)$.*

Using this, Krajíček and Oliveira [11] showed that

Theorem 14 (Krajíček and Oliveira [11]) *For any $k \in \omega$ there exists $L \in P$ such that $L \notin Size(n^k)$ is consistent with PV.*

It is unknown whether a similar separation holds for PSPACE and Boolean programs. So it would be interesting to start with the ground models which satisfies or negates the condition

$$PSPACE \subseteq BP_k$$

and study their generic extension.

Specifically, we can formalize the statement of Theorem 13 as

$$SW_k(n) \equiv \forall c\, \exists X \in BP_n\, \forall Y \in BP_n(|Y| \leq cn^k \rightarrow X \neq_{BP} Y).$$

Let $\mathfrak{M} \models W_1^1 + \neg SW_k(n)$ for some $k \in \omega$. Then by Theorem 12, any TY-genric $\mathbb{G}$ is a member of $\mathfrak{M}[\mathbb{G}]$.

Now suppose we have some combinatorial principle expressed by three-sort formula, say $\forall \mathcal{S}\ \Phi(\mathcal{S})$ which is either true, false or even cannot be decided in the standard model. If we can construct some ideal $\mathbb{I}$ such that

$$\mathfrak{M}[\mathbb{G}] \models \neg\Phi(\mathbb{G})$$

where $\mathbb{G}$ is a TY-genric over $\mathbb{I}$ then we have

$$\mathbf{QBFV} \nvdash \forall \mathcal{S}\ \Phi(\mathcal{S}).$$

It is an interesting problem to find a natural combinatorial principle which is expressed by such $\Phi(\mathcal{S})$.

5.2 Separation problems and generic extensions

We can show that the separation condition for P and $PSPACE$ affects the strength of the generic extension. Namely, let $\mathbb{B}_C$ be the Boolean algebra which consists of circuits in $\mathfrak{M}$. Then we can construct generic extension in the same manner as for $\mathbb{B}_{BP}$ and show that $\mathfrak{M}[\mathbb{G}]$ is a model of the three-sort conservative extension of PV. Moreover, we have the followings:

Theorem 15 *If $\mathfrak{M} \models W_1^1 + P = PSPACE$ then $\mathfrak{M}[\mathbb{G}] \models$ **QBFV** for any TY-generic $\mathbb{G} \in \mathbb{B}_C$.*

Theorem 16 *If $\mathfrak{M} \models W_1^1 + P \neq PSPACE$ then $\mathfrak{M}[\mathbb{G}] \models$ **QBFV** for some TY-generic $\mathbb{G} \in \mathbb{B}_C$.*

On the other hand, it seems much harder to show that generic extension for $\mathbb{B}_{BP}$ satisfies or excludes $\Sigma_1^{\mathcal{B}}$ induction.

Problem 1 *Prove or disprove that if $\mathfrak{M} \models W_1^1 + PSPACE = EXPTIME$ then*

$$\mathfrak{M}[\mathbb{G}] \models \Sigma_1^{\mathcal{B}}\text{-}IND$$

for any TY-generic $\mathbb{G}$.

Problem 2 *Prove or disprove that if* $\mathfrak{M} \models W_1^1 + PSPACE \neq EXPTIME$ *then*

$$\mathfrak{M}[\mathbb{G}] \not\models \Sigma_1^{\mathcal{B}}\text{-}IND$$

for some TY-generic $\mathbb{G}$.

In general, the problem of whether the generic extension satisfies axiom schemata for $\Sigma_1^{\mathcal{B}}$ formulas is difficult. This is mainly because we have forcing theorem only for $\Sigma_0^{\mathcal{B}}$ formulas. So we need neat techniques to treat $\Sigma_1^{\mathcal{B}} \cup \Pi_1^{\mathcal{B}}$ formulas in the generic extension.

Concerning the separation of $EXPTIME$ from $PSPACE$, we can prove the followings:

Theorem 17 *If* $\mathfrak{M} \models W_1^1 + EXPTIME = PSPACE$ *then* $\mathfrak{M}[\mathbb{G}]$ *is closed under* $EXPTIME$ *functions for any TY-generic* $\mathbb{G} \in \mathbb{B}_{BP}$.

Theorem 18 *If* $\mathfrak{M} \models W_1^1 + EXPTIME \neq PSPACE$ *then* $\mathfrak{M}[\mathbb{G}]$ *is not closed under* $EXPTIME$ *functions for some TY-generic* $\mathbb{G} \in \mathbb{B}_{BP}$.

5.3 Generic extensions for other classes

In principle, if we can define Boolean algebras for complexity classes other than PSPACE, we can construct generic extensions which are models of some minimal theory for the class.

An example for such a class is EXPTIME. Actually, we can define a Boolean algebra which consists of succinct Boolean circuits and show that the generic extension satisfies the axiom stating that any succinct circuit can be evaluated.

Another interesting case is counting classes. However, we do not even know any theory for counting classes.

Problem 3 *Define a three sort theory for the class* $FP^{\#P}$. *Also define a Boolean algebra for the class.*

References

[1] M. Ajtai. The complexity of the pigeon hole principle. In Proceedings of IEEE 29th Annual Symposium on Foundations of Computer Science, (1988). pp. 346–355.

[2] A. Atserias, M. Müller, Partially definable forcing and bounded arithmetic. Archive for Mathematical Logic 54 (1) (2015) pp.1–33.

[3] S.R.Buss, Bounded arithmetic. PhD Thesis (1985).

[4] S.R.Buss, Relating the Bounded Arithmetic and Polynomial Time Hierarchies. Annals of Pure and Applied Logic, 75 (1995) pp.67–77.

[5] P.Clote and G.Takeuti, First Order Bounded Arithmetic and Small Boolean Circuit Complexity Classes. Feasible Mathematics II, Springer, (1995). pp.154–218.

[6] S.A.Cook, Feasibly constructive proofs and the propositional calculus (Preliminary Version). Proceedings of the 7th Annual ACM Symposium on Theory of Computing, (1975), pp.83–97.

[7] S.A.Cook and P.Nguyen, Logical foundations of proof complexity. Perspectives in Logic. Cambridge University Press, New York, (2010).

[8] J.Krajíček, P. Pudlák and G. Takeuti: Bounded Arithmetic and the Polynomial Hierarchy. Annals of Pure and Applied Logic, 52, (1991), pp. 143–153.

[9] J.Krajíček, "On Frege and Extended Frege Proof Systems", in: "Feasible Mathematics II", eds. P. Clote and J. Remmel, Birkhauser, (1995), pp. 284–319.

[10] J.Krajíček, Extensions of models of PV, in: Logic Colloquium'95, Eds. J.A.Makowsky and E.V.Ravve, ASL/Springer Series *Lecture Notes in Logic*, Vol. **11**, (1998), pp.104–114.

[11] J.Krajíček, I.C.Oliveira, Unprovability of circuit upper bounds in Cook's theory PV, Logical methods in Computer Science, Volume 13, Issue 1, (2017).

[12] S.Kuroda, Sprague-Grundy theory in bounded arithmetic. submitted.

[13] M. Müller, Typical forcing, NP search problems and an extension of a theorem of Riis. Preprint.

[14] J.B. Paris and A. Wilkie, Counting problems in bounded arithmetic, Methods in Mathematical Logic, LNM 1130, Springer Verlag, (1985) pp.317–340

[15] S.Riis, Finitisation in Bounded Arithmetic : Slightly extended version of: Making infinite structures finite in models of Second Order Bounded Arithmetic.In: Arithmetic, proof theory and computational complexity, Oxford University Press (1993) pp.289–319

[16] A.Skelley, Theories and Proof Systems for PSPACE and the EXP-Time Hierarchy. PhD thesis, Toronto Unversity. (2006)

[17] R.Santhanam and R.Williams, On Uniformity and Circuit Lower Bounds. Computational Complexity, 23, (2014), pp.1771-205

[18] G.Takeuti and M.Yasumoto, Forcing on Bounded Arithmetic. in:Gödel '96, Lecture Notes in Logic, vol.6, (1996) pp.120–138.

[19] G.Takeuti and M.Yasumoto, Forcing on Bounded Arithmetic II. Journal of Symbolic Logic, Volume 63, Issue 3 (1998), pp.860–868.

[20] D.Zambella, Notes on Polynomially Bounded Arithmetic. Journal of Symbolic Logic, Volume 61, Issue 3 (1996), pp.942–966.

群馬県立女子大学　黒田覚